Risoluzione dei problemi di connettività con Sourcefire User Agent

Sommario

Introduzione

Sourcefire User Agent esegue il monitoraggio dei server Microsoft Active Directory e segnala gli accessi e le disconnessioni autenticati tramite LDAP. Il sistema FireSIGHT integra questi record con le informazioni che raccoglie attraverso l'osservazione diretta del traffico di rete da parte dei dispositivi gestiti. Quando si utilizza Sourcefire User Agent, potrebbero verificarsi problemi tecnici. In questo documento vengono forniti suggerimenti per la risoluzione di vari problemi relativi a Sourcefire User Agent.

Prerequisiti

Cisco raccomanda la conoscenza di FireSIGHT Management Center, Sourcefire User Agent e Active Directory.

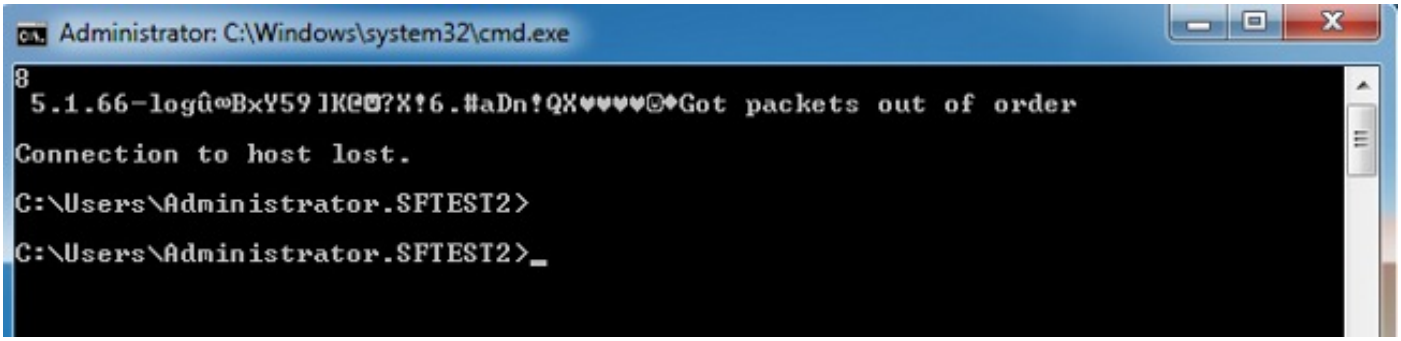
> Suggerimento: per ulteriori informazioni sull'installazione e la disinstallazione di Sourcefire User Agent, leggere questo documento.

Problemi di connettività

1. Verificare che l'agente utente sia stato aggiunto al centro di gestione FireSIGHT. Per verificare questa condizione, passare a Criteri > Utenti > Agente utente e verificare che l'indirizzo IP dell'host dell'agente utente configurato sia corretto.
2. Confermare che la porta 3306 sia aperta e in ascolto. Non sono presenti firewall o altri dispositivi di rete che impediscono all'agente utente di comunicare con il Centro difesa.
3. La porta 3306 non sarà aperta finché non sarà stata configurata una voce Agente utente nel centro di gestione FireSIGHT.

4. Se su un host dell'agente utente è installato telnet, è possibile verificare la connessione mediante telnet dall'host dell'agente utente al centro di gestione FireSIGHT. Viene visualizzato il log 5.1.66 seguito da una stringa di caratteri ASCII. Premere CTRL+C più volte per disconnettersi.

Nota: è previsto l'aspetto del messaggio Pacchetti ricevuti non in ordine.



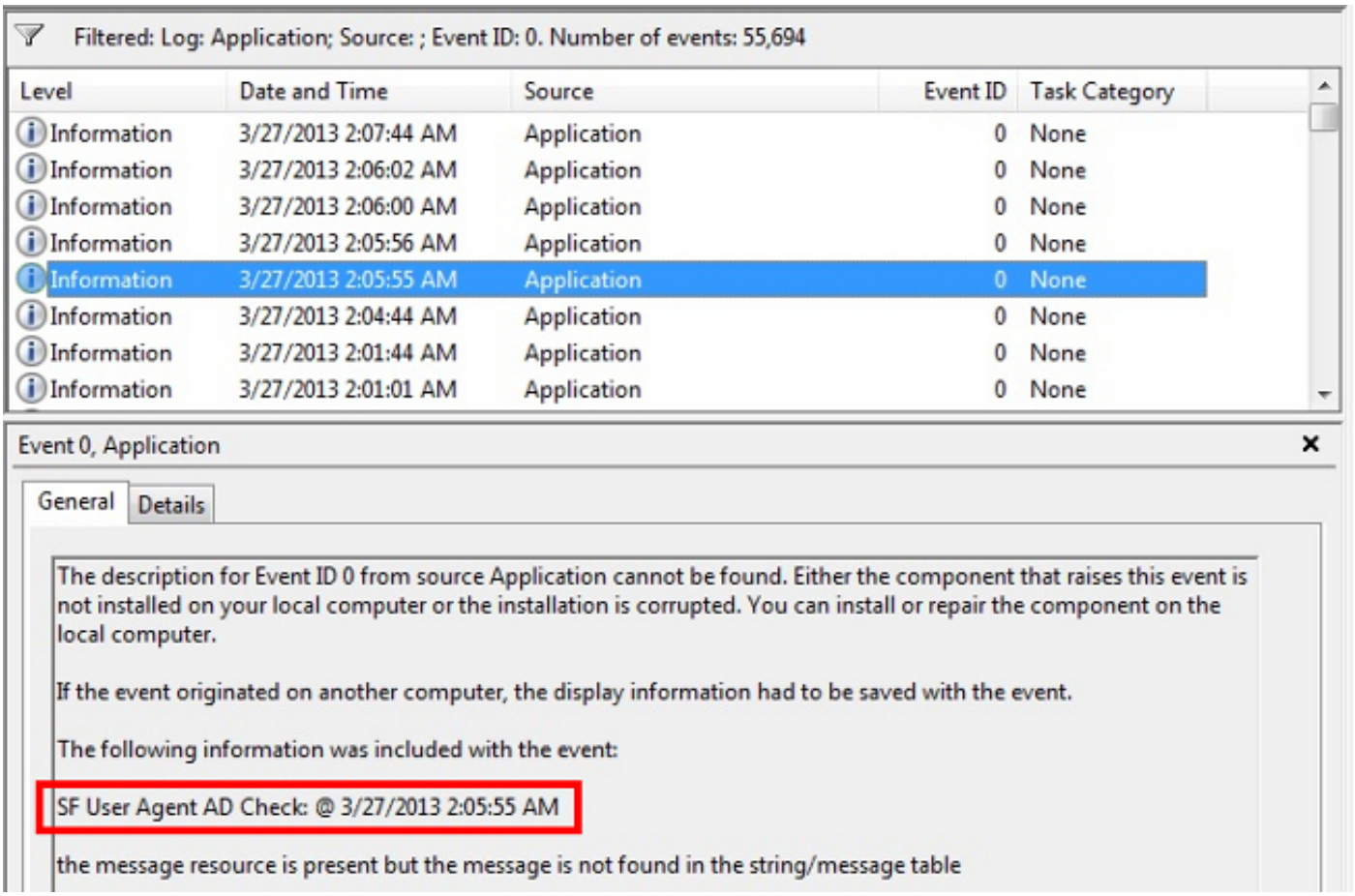
Se l'agente utente genera errori durante la connessione o l'autenticazione ai server Active Directory, è possibile che si sia verificato un problema di autorizzazioni per account utente o di rete. Verificare che non vi siano problemi di connettività di rete nell'ambiente e configurare temporaneamente l'agente utente in modo che utilizzi un account di amministratore di dominio per l'autenticazione nei server Active Directory per il test, se possibile.

Registrazione diagnostica

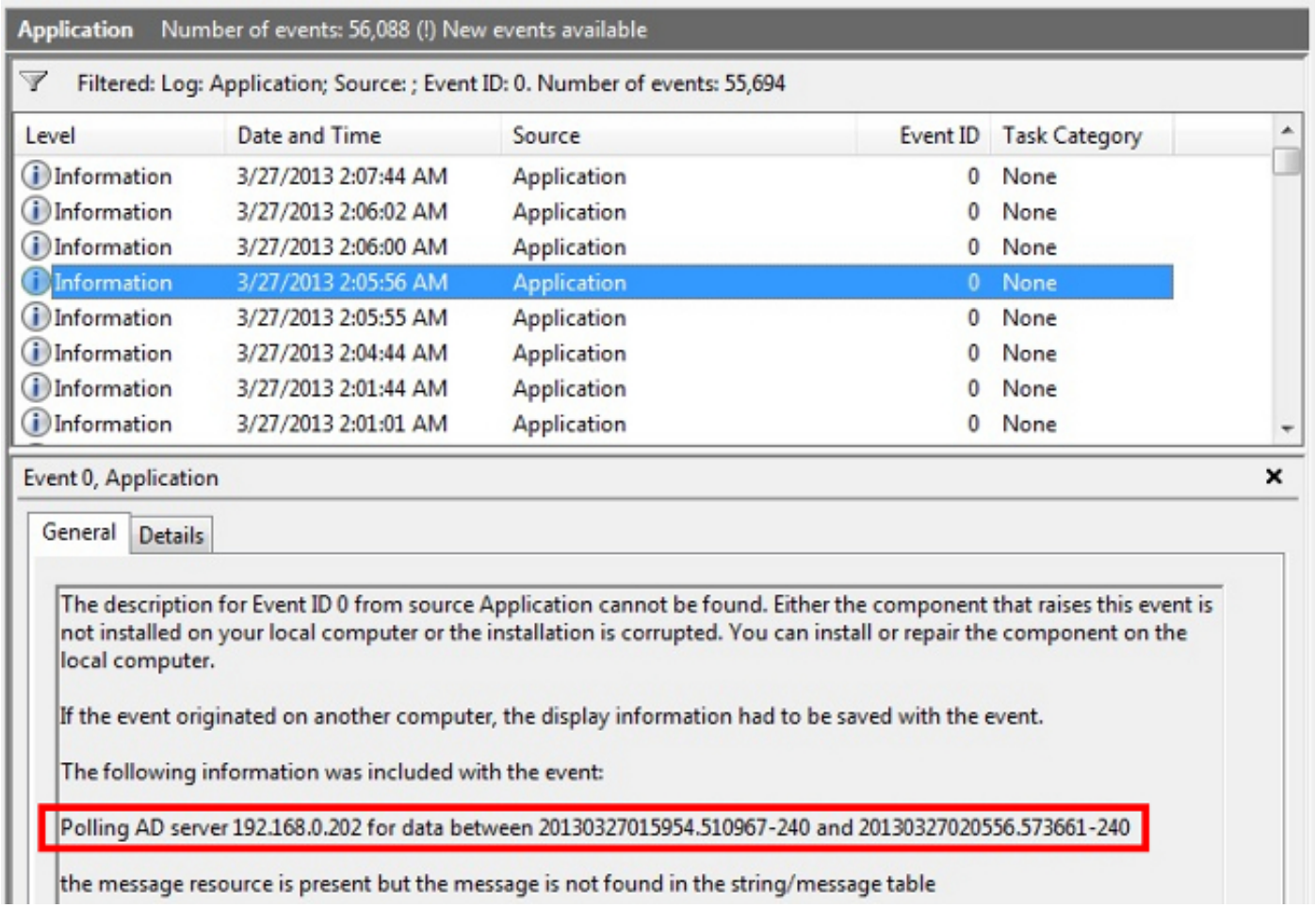
Per la risoluzione dei problemi generali dell'agente utente, selezionare Log to local event log within the User Agent GUI client e fare clic su Save. In questo modo, nel registro eventi dell'applicazione host dell'agente utente verranno immessi utili messaggi operativi. È possibile verificare che il polling dell'agente utente sia stato completato correttamente cercando i seguenti eventi nell'ordine indicato:

Nota: le schermate seguenti sono tratte dal Visualizzatore eventi Microsoft sull'host su cui è in esecuzione l'agente utente.

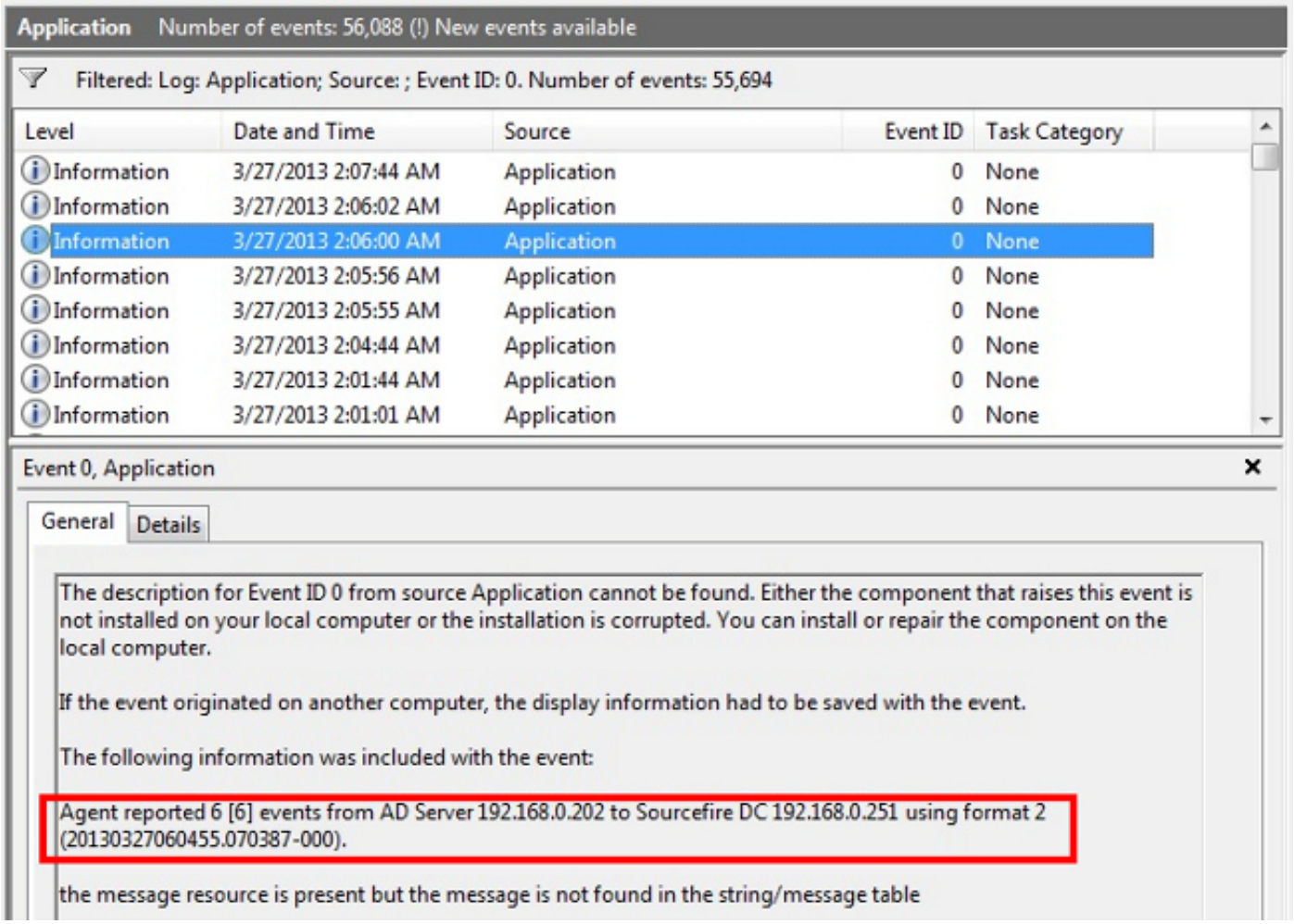
Controllo Active Directory agente utente



Agente utente che esegue il polling del server Active Directory



Numero di eventi segnalati dall'agente (#) al Centro difesa


Application Number of events: 56,088 (!) New events available
Filtered: Log: Application; Source: ; Event ID: 0. Number of events: 55,694
Level Date and Time Source Event ID Task Category
Information 3/27/2013 2:07:44 AM Application 0 None
Information 3/27/2013 2:06:02 AM Application 0 None
Information 3/27/2013 2:06:00 AM Application 0 None
Information 3/27/2013 2:05:56 AM Application 0 None
Information 3/27/2013 2:05:55 AM Application 0 None
Information 3/27/2013 2:04:44 AM Application 0 None
Information 3/27/2013 2:01:44 AM Application 0 None
Information 3/27/2013 2:01:01 AM Application 0 None
Event 0, Application
General Details
The description for Event ID 0 from source Application cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.
If the event originated on another computer, the display information had to be saved with the event.
The following information was included with the event:
Agent reported 6 [6] events from AD Server 192.168.0.202 to Sourcefire DC 192.168.0.251 using format 2 (20130327060455.070387-000).
the message resource is present but the message is not found in the string/message table

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).